»Ihr Auto wurde gehackt! Zahlen Sie!! Oder Ihre Bremsen versagen!!!« Die neue Bedrohung?

Selbstfahrende Autos sollen den Straßenverkehr komfortabler machen. Experten diskutieren die Gefahren VON ANJA REITER

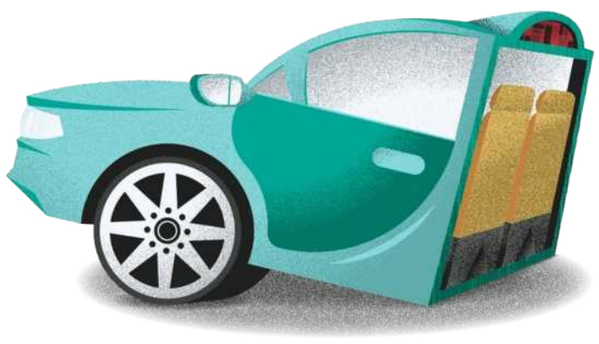

Illustration: Bastian Kamp für DIE ZEIT

Ein fahrerloses Roboterauto donnert über die Stadtautobahn. Der einzige Passagier, ein müder Manager, döst auf der Rückbank dem Feierabend entgegen. Plötzlich wird er unsanft aus dem Schlaf gerissen: Krachend startet die Musikanlage, wie von Zauberhand öffnet sich das Schiebedach. Auf dem Bordbildschirm blinkt eine Nachricht auf: *»System hacked!!«* Die Drohung der Hacker: Nur wenn der Geschäftsmann das nötige Lösegeld in Form von Bitcoins bezahlt, kommt er mit seinem Leben davon.

Noch sind Cyberattacken wie diese auf unseren Straßen unvorstellbar. Bei einschlägigen Konferenzen werden solche Szenarios aber bereits diskutiert. Moderne Autos sind schon heute rollende Computernetzwerke – mit jeder Menge Elektronik, USB-Schnittstellen und drahtlosen Verbindungen an Bord. Die Fahrzeugcomputer rufen aktuelle Verkehrsprognosen ab, ziehen Musik von Streamingportalen oder zapfen das Netz für Software-Updates an. Wenn Autos erst autonom unterwegs sind, schreitet diese Form der Vernetzung weiter voran.

Das Problem: Alle Daten, die aus dem Auto oder in das Auto kommen, geben Hackern Angriffspunkte.

> Der Angriff auf ein Auto gelingt über Verbindungen wie Bluetooth

Die Politik hat die Gefahr mittlerweile erkannt. Das Bundesforschungsministerium fördert Projekte zur IT-Sicherheit des autonomen und vernetzten Fahrens. Unternehmen wie Bosch und Volkswagen sitzen mit der Universität Tübingen an einem Projekt, das bereits in der Entwicklung von autonomen Fahrzeugen Hacking-Gefahren mindern soll. Wo sind die gefährlichsten Schwachstellen – und was wird von den Herstellern heute schon getan, um Hacker-Angriffe zu verhindern?

Stefan Nürnberger, 32, hat selbst mehrere Autos gehackt. Der Informatiker und Experte für IT-Sicherheit ist ein sogenannter White-Hat-Hacker. Ihn treibt keine kriminelle Energie an, sondern der wissenschaftliche Ehrgeiz. Am Helmholtz-Zentrum für Informationssicherheit in Saarbrücken tüfteln Nürnberger und seine Kollegen so lange an der IT-Infrastruktur eines Autos, bis sie Einfallstore finden. Durch das Aufdecken von solchen potenziellen Fehlern möchten sie die allgemeine Sicherheit erhöhen. Welche Automarken er bisher geknackt hat, will Nürnberger nicht verraten. Nur so viel: Häufig gelinge der Angriff über fehlerhafte Funkverbindungen. Wenn etwa Bluetooth nicht richtig programmiert sei, könne man über das Smartphone Schadsoftware einschleusen und so den Computer im Auto aus dem Tritt bringen. »Ganz ähnlich wie bei Viren in PDF-Dateien.«

Wie anfällig ein Fahrzeug für die digitale Manipulation ist, hängt stark vom Hersteller ab – und von der spezifischen Sicherheitsarchitektur des Autos. »Im schlimmsten Fall kann man über das Infotainment-System bis zu den sicherheitsrelevanten Funktionen des Autos vordringen«, erklärt Nürnberger. Dann sei die »feindliche Übernahme« komplett. Zwar sei das Vordringen bis zur Servolenkung oder gar zur Bremse komplex, für kriminelle Hacker mit dem nötigen Know-how sei das aber bei manchen Modellen machbar.

Doch werden solche IT-Lücken von Kriminellen auch bereits erschlossen? »Noch existiert zum Glück kein Geschäftsmodell, um Fahrzeuginsassen, Hersteller oder Flottenbetreiber durch das Ausnutzen von Sicherheitslücken zu erpressen«, sagt Nürnberger. Für die Zukunft gibt es jedoch viele bedrohliche Szenarios: eine Schadsoftware, die den Tankdeckel oder die Bremse blockiert und für deren Freigabe Lösegeld fordert. Taxiflotten, die lahmgelegt oder fehlgeleitet werden. Terroristische Angriffe auf die vernetzte Verkehrsinfrastruktur einer Stadt. Der Fantasie sind keine Grenzen gesetzt.

Deutsche Autohersteller halten die Risiken von Hacker-Angriffen derweil für gering. In München-Unterschleißheim hat sich im vergangenen Jahr das Kompetenzzentrum für autonomes Fahren der BMW-Gruppe niedergelassen. 1300 Mitarbeiter werkeln auf dem Campus am Traum des fahrerlosen Autos, unter ihnen Maschinenbauer, Informatiker, Datenwissenschaftler, Psychologen und Kryptografen. Während Projektteams namens MacGyver oder Leibniz zwischen Whiteboards neue Codes entwickeln, drehen draußen die autonomen Testwagen ihre Runden. Sie sammeln reale Verkehrsdaten, mehrere Millionen Gigabyte pro Tag.

Dirk Wisselmann, Maschinenbauingenieur und BMW-Referent in der Entwicklung für automatisiertes Fahren, glaubt nicht daran, dass von kriminellen Hackern irgendwelche Horrorszenarien verursacht werden könnten: »Die individuelle Gefahr für den Einzelnen ist meiner Ansicht nach eher gering.« Bei BMW sorge eine eigenständige Elektronik-Architektur mit verschiedenen Schutzmechanismen dafür, dass Hacker kein leichtes Spiel haben. Software werde aufwendigen Tests unterzogen, die Zahl der Schnittstellen reduziert. »Das verlagert einen Angriff auf die Ebene von absoluten Experten«, sagt Wisselmann. Sollte es in Zukunft dennoch Angriffe geben, würden sich diese zudem eher gegen den Konzern richten und nicht gegen den einzelnen Autofahrer.

Dass aber auch BMW-Autos über Sicherheitslücken verfügen, bewiesen im vergangenen Jahr IT-Experten aus China: Bei einer Analyse der Fahrzeug-Software fanden die Experten des Tencent Keen Security Lab insgesamt 14 Sicherheitslücken in unterschiedlichen BMW-Modellen, so im Infotainment-System oder beim USB-Zugang. Über einen gehackten Mobilfunkzugang konnten die Chinesen sogar Befehle auf den zentralen Kabelstrang im Auto senden, der alle Fahrzeugkomponenten miteinander verbindet. Mittlerweile hat BMW diese Lücken nach eigener Aussage geschlossen.

Bleibt die Frage, ob Autohersteller sich aufgrund solcher IT-Sicherheitsrisiken nicht lieber gänzlich von der Idee des vernetzten und voll automatisierten Verkehrs verabschieden sollten.

Das halten jedoch selbst Maschinenethiker wie Matthias Uhl von der Hochschule für Politik in München für unsinnig. »Derzeit sterben weltweit Hunderttausende Menschen pro Jahr, weil sie betrunken oder übermüdet hinter dem Steuer sitzen.« Autonomes Fahren könne diese menschliche Fehlbarkeit als Risikofaktor ausschalten oder zumindest verringern. »Im Grunde tauschen wir viele kleine Einzelrisiken gegen ein großes Risiko ein: die Idee eines großen Hacking-Angriffs.«

IT-Experte Nürnberger ist sich sicher, dass für ambitionierte Hacker immer Einfallstore bleiben werden. »Eine hundertprozentige Sicherheit ist nicht möglich.« Gerade deshalb müssten Automobilkonzerne die Risiken minimieren und schleunigst ihre über Jahrzehnte gewachsene Sicherheitsarchitektur über den Haufen werfen und für das autonome Fahren neu aufbauen. Diese teure Investition müsste freilich an den Kunden weitergereicht werden. Das Problem dabei? »Während man seinem Kunden einen Massagesitz demonstrieren kann, ist das bei IT-Sicherheit schwieriger.«

Nürnberger ärgert sich einstweilen über die fehlende Kooperationsbereitschaft der Automobilindustrie. Wollten er oder seine Kollegen die Ergebnisse eines Hacking-Tests veröffentlichen, werde ihnen mitunter mit Klage gedroht. Vor einigen Monaten veröffentlichte sein Team ein Softwarepaket, das Hacker-Angriffe durch interne Authentifizierungscodes abwehren kann. Die Software VatiCAN ist frei im Internet verfügbar, Unternehmen können damit ihre Fahrzeuge nachrüsten. Das Interesse der Konzerne? »Null.«

Nürnberger blickt da schon lieber in die USA. »Die amerikanischen Hersteller Tesla und GM sind momentan die einzigen, die vernünftig mit der Hacking-Bedrohung umgehen, indem Kunden Sicherheitslücken melden können«, sagt Nürnberger.

Tesla arbeitet schon seit vielen Jahren mit den White-Hat-Hackern zusammen und verspricht ihnen lukrative Prämien: In der Vergangenheit konnten Hacker ein aktuelles Tesla-Modell gewinnen, wenn sie Sicherheitslücken fanden – oder sie erhielten gleich ein Jobangebot des amerikanischen Herstellers.

Maschinenethiker Uhl glaubt, dass es in Zukunft ein permanentes Wettrüsten zwischen Herstellern und Hackern geben werde, ähnlich wie bei der Schadsoftware für PCs: Hacker suchen nach Lücken im System, die Industrie schließt sie. »Bisher haben die Ingenieure gegen die Natur gearbeitet«, sagt er. »Jetzt arbeiten sie gegen eine kriminelle Intelligenz.«

www.zeit.de/audio